METHOD FOR PROVIDING AND BILLING WIM FUNCTIONALITIES IN MOBILE COMMUNICATION TERMINALS

[0001] The invention relates to a method for providing and billing WIM functionalities in mobile communication terminals.

State of the Art

[0002] An open standard called WTLS (Wireless Transport Layer Security) was developed by mobile network operators and device manufacturers for secure electronic transactions via the mobile phone network. WTLS is based on existing standards like WAP (Wireless Application Protocol) and TLS (Transport Layer Security) for encoding and WIM (Wireless Identification Module) for identification and signature. TLS or WTLS technology concerns a protocol of the transport layer. This layer innately ensures a reliable, transparent, and encoded transmission of data between two systems based on a so-called public key infrastructure (PKI). Moreover, it functions like an interface between the above-lying application-oriented layers and the lower-lying network-oriented layers. The central task is the formation of a connection and the control between two processes. The identification and signature of the information takes place via the WIM. Signatures that take place during the handshake in the WLTS/TLS are not initiated by the user and occur automatically. A separate key is also used here that is not the signature key that is used for signatures within applications.

[0003] This allows various transactions to be performed with mobile communication terminals, like e.g. bank and stock exchange transactions, credit card and other payments, as well as access control to buildings and computers. Together with suitable infrared interfaces or the short-distance radio communications standard "Bluetooth," payments are possible in connection with points of sale and gas pumps as well as authorizations at lock systems.

[0004] The necessary PKI procedures are performed individually between a subscriber (customer) and any service provider, whereby the subscriber registers as appropriate with the service provider. The WIM on the other hand is generally provided by the operator of the communication network used by the end device and is realized in an end device or an identification module, e.g. SIM, connected with it.

Object of the Invention

[0005] The object of the invention is to suggest a method that allows the simple and secure provision and billing of WIM functionalities in mobile communication terminals.

[0006] This object is solved according to the invention through the characteristics of patent claim 1.

[0007] Advantageous embodiments and advanced versions of the invention are given in the dependent patent claims.

[0008] It is suggested that the number of WIM signatures that can be performed by an end terminal or an identification module, e.g. an SIM chip card, be limited using a counter. The counter counts each signature. When the counter reaches a threshold value, no more signatures are allowed until a reset has taken place via a type of release / reload.

[0009] In accordance with the invention, the WIM provides functionality with which signatures can be created on the application level. These are initiated by the subscriber (user); the subscriber must e.g. enter his/her so-called PIN-NR (non-repudiation PIN) for each signature.

[0010] The WIM blocks the "signing" functionality when the counter has run out. A release/reloading can then e.g. take place via OTA (over the air message) and be billed to the subscriber.

[0011] An exemplary embodiment of the invention is described below. A mobile telephone with an identification module (SIM card) with devices for implementing secure electronic transactions and corresponding interfaces is assumed to be the mobile communication terminal.

[0012] The WIM internally counts each signature initiated by the subscriber. When a preset number of signatures have been performed, no further signatures are possible until this function has been released again. The release occurs via the air interface of the mobile communication network (over the air) using a corresponding SAT application (SAT: SIM Application Toolkit) implemented on the SIM card and can only take place via the network operator. At the same time as the release, the number of possible can be reset. A counting of each individual signature in the mobile communication network is not required.

[0013] Various options are possible and can be combined:

- The signature can generally be released, e.g. for post-paid subscribers, i.e. subscribers with SIM card contracts or subscribers who pay a higher base fee.
- The counter reading on the card can be queried by the subscriber locally via a simple SAT function, e.g. to request the release of additional signatures in advance, e.g. via an SAT function. The release is charged/billed to the subscriber.

- After the last signature has been used, the card sends an SMS to a central device connected to the communication network, e.g. a release server, which bills the number of used signatures to the subscriber and then releases the signature functionality again, if the subscriber wishes (can be used for prepaid and post-paid).

[0014] The internal counter counts down with each signature. The WIM function is blocked when the counter reading = 0. A release takes place "over the air" e.g. via an SAT application. An unlimited signing can e.g. be released if the network operator sets the reading on the counter to a value of -1.

[0015] The invention allows third parties, e.g. banks, to create their own PKI procedures and to register their own subscribers for the use of these procedures. The network operator does not need its own PKI procedures, but rather makes available to the subscribers a universally usable WIM.